boxes, and numerous reconnection dialog boxes. In the case that the user has not connected to the certificate manager, an input screen for the user password is displayed. The dial-up client (120) allows for the termination of a session via a cancel button on the connection information dialog box. Each service provided by the Remote Access Switch (110) to a dial-in user constitutes a session, with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. In the case of abnormal termination of the session, the dial-up client (120) automatically displays a reconnection dialog box to allow the user to re-establish the session. The dial-up client (120) also announces a desire to use SDAP before any other authentication protocols.

[0049] A typical phone number and modem setup dialog box, in accordance with one or more embodiments of the present invention, is shown in Figure 4. A dialog box (52) contains a listing of phone book entries (54) associated with phone numbers to access a remote server. The dialog box (52) also contains a button to add a phone book entry (60), a button to remove a phone book entry (62), and a button to edit a phone book entry (58). Further, the dialog box (52) contains a button to dial the phone number associated with a selected phone book entry (56).

[0050] A typical connection information dialog box, in accordance with one or more embodiments of the present invention, is shown in Figure 5. A dialog box (64) informs the user of the progress of the connection. The dialog box (64) includes a text dialog (65) that indicates the current state of the dialing/authentication process. Additionally, the dialog box (64) contains a cancel button (66) that may be used to terminate the connection at any time during the dialing/authentication process.

[0051] A typical input dialog box for a user name and password, in accordance with one or more embodiments of the present invention, is shown in Figure 6. A

dialog box (68) contains a drop-down text input field (70) to select a user profile name and a text input field (72) to enter a user password. Once the user has entered both the user profile name and password, an OK button (74) may be clicked to continue the dialing/authentication process.

[0052] A typical error dialog box, in accordance with one or more embodiments of the present invention, is shown in Figure 7. A dialog box (76) contains a text message field (78) indicating an error that was encountered. An OK button (80) may be clicked to continue running the SmartDial application.

[0053] The PKI-Bridge (124) resides on the server (112) and uses the RADIUS Software Development Kit (SDK). The PKI-Bridge (124) is the interface on the server (112) that supports the integration of the server (112) and the server-side cryptographic function (130), for CHAP authentication. The PKI-Bridge (124) forwards a challenge string from the server-side cryptographic function (130) to the client computer (102).

[0054] Further, the PKI-Bridge (124) reconstructs the signed response packets, sent from the client computer (102) and forwards them to the server-side cryptographic function (130). The signed response string is verified by the server-side cryptographic function (130). If the verification is successful, the server (112) is instructed, by the server-side cryptographic function (130) via the PKI-Bridge (124), to send an allow connection message to the Remote Access Switch (110). If the verification is unsuccessful, the server (112) is instructed, by the server-side cryptographic function (130) via the PKI-Bridge (124), to send a deny connection message to the Remote Access Switch (110). For security purposes, the PKI-Bridge (124) does not store the challenge string or the signed response. The PKI-Bridge (124) constructs a random string of characters for the challenge string based on a timestamp, the previous response, and a randomly generated

number. The challenge string is only valid for one session and times out after a configurable time period.

[0055] In an embodiment of the present invention, the client-side cryptographic function (128) and the server-side cryptographic function (130) are developed by the same vendor and employ the same cryptographic scheme.

[0056] In another embodiment of the present invention, the client-side cryptographic function (128) and the server-side cryptographic function (130) are developed by different vendors and employ the same cryptographic scheme.

[0057] Referring to Figure 8, a typical implementation of SmartDial starts with a user attempting to dial into the Remote Access Switch (110) (Step 140). If the attempt to connect to the Remote Access Switch (110) is unsuccessful (Step 142), a dialog box appears to ask whether to retry the attempt to dial into the Remote Access Switch (110) (Step 144). If the user chooses not to retry, SmartDial terminates (Step 164). If the user chooses to retry, a dialog box for determining whether the same access number should be used appears (Step 146). If the user chooses the same access number, the process starts again with an attempt to dial into the Remote Access Switch (110) (Step 140). If the user chooses not to use the same number, an alternate number is then selected by the user (Step 148) and the process starts again with an attempt to dial into the Remote Access Switch (110) (Step 140).

[0058] If the attempt to connect to the Remote Access Switch (110) is successful (step 142), the client computer (102) requests a SmartDial authentication through the Remote Access Switch (110) to the server (112) (Step 150). In one embodiment of the present invention, the request and all the subsequent data transmission between the client computer (102) and the Remote Access Switch (110) is conducted via a hidden terminal using a 64-bit encoding. The SmartDial system proceeds to authenticate the dial-up user (Step 151). If authentication is